обходимость применения средств мониторинга функционирования систем диспетчерского контроля и разработка комплекса инженерно-технических и организационных мер, препятствующих реализации хотябы наиболее вероятных сценариев атак.

Список литературы

1. *Пищик Б. Н.* Безопасность АСУ ТП // Вычислительные технологии. Спец. выпуск. 2013. Т. 18. С. 170–175.

2. *Шахновский Г.* Безопасность Систем SCADA и АСУТП. URL: http://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/bezopasnost_sistem_scada_i_asutp (дата обращения: 13.02.2016).

3. *Агафонов А. В.*, *Синадский Н. И.* Тестирование защищенности телекоммуникационного оборудования от сетевых компьютерных атак типа «отказ в обслуживании» с применением генетического алгоритма // Вестн. УрФО. Безопасность в информационной сфере. 2017. № 2 (24). С. 4–9.

4. *Лукацкий А.* Стандарты безопасности АСУ ТП. URL: http://www.slideshare.net/CiscoRu/ss-8690963 (дата обращения: 20.06.13).

УДК 004.056.53

В. В. Шмелёв
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

УЯЗВИМОСТИ РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ

Аннотация. В настоящей статье рассмотрены проблемы уязвимости рабочих станций и серверов. Данное исследование имеет целью выработку рекомендаций, направленных на предотвращение уязвимостей. По сравнению с аналогичными исследованиями, результатами данной работы являются рекомендации, соблюдая которые существенно снижается риск успешной атаки злоумышленников на рабочие станции и сервера.

Ключевые слова: уязвимость; рабочая станция; сервер; пароль; межсетевой экран; администратор; пользователь; обновление.

Значение информации в нашем современном мире можно охарактеризовать известной фразой Натана Ротшильда: «Кто владеет информацией, тот владеет миром». С ростом ценности информации появляется большее количество заинтересованных людей третьих лиц, стремящихся получить несанкциониро-

ванный доступ к ценной информации. Чаще всего целями этих злоумышленников является информация, нарушение конфиденциальности которой может принести злоумышленникам прибыль. Данная информация обычно обрабатывается в организации на рабочих станциях и серверах, и для ее получения злоумышленники используют уязвимости рабочих станций и серверов.

Актуальность данной статьи объясняется тем, что информационные технологии, обрабатывающие ценную информацию, довольно широко используются различными организациями, и для сохранения конфиденциальности, целостности и доступности информации необходимо устранить уязвимости, позволяющие реализовать успешную атаку на рабочие станции или сервера.

Для уточнения толкования ряда понятий им необходимо дать определения.

Рабочая станция — это вычислительная машина в составе локальной вычислительной сети по отношению к серверу. Чаще всего под рабочими станциями подразумевают офисные персональные компьютеры, используемые для работы с профессиональными научными и инженерными приложениями, разработки программного обеспечения и приложений. Особо выделяют специализированные графические рабочие станции для работы с трехмерной графикой.

Сервер — специализированный компьютер, выполняющий определенные функции по запросам рабочих станций, других серверов и различных цифровых устройств, подключенных к данной сети. Сервер является системообразующим компонентом той сети или того сегмента сети, за который он отвечает. Через него передаются данные от одной рабочей станции к другой или к другому серверу. В небольших сетях роль сервера может выполнять одна из рабочих станций, в глобальных сетях для одной и той же функции может использоваться несколько серверов.

В информационной безопасности термин «уязвимость» используется для обозначения недостатка в системе, используя который можно намеренно нарушить ее целостность и вызвать неправильную работу.

На данном этапе необходимо рассмотреть уязвимости рабочих станций и серверов.

Самая распространенная уязвимость — слабый пароль. Пароль является основным способом определения подлинности пользователя. Плохой пароль или его отсутствие ставит под угрозу информационную безопасность, так как злоумышленник может использовать подбор пароля с помощью специальных программ или же с помощью знаний каких-либо фактах о владельце и получить неограниченный доступ к ресурсам рабочей станции или сервера.

Открытый доступ к настройкам BIOS тоже является опасной уязвимостью в том случае, если у потенциального злоумышленника может быть физический доступ к рабочей станции. Изменив настройки, преступник может навредить

работоспособности рабочей станции или же получить доступ к данным компьютера в обход парольной защиты, используя носитель с операционной системой.

Неправильная настройка или отсутствие межсетевого экрана открывает множество возможностей для сетевых атак рабочих станций и серверов извне. Межсетевой экран (англ. *firewall*) — это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Используя уязвимости неправильно настроенного межсетевого экрана злоумышленник может в рамках разрешенного протокола реализовать атаку.

Использование посторонних устройств негативно влияет на защиту информации. Даже правильно настроенный межсетевой экран не сможет защитить сеть, если трафик, использующий «бреши» в защите, не проходит через него. Это возможно реализовать при использовании на компьютере, к примеру, USB-модема. Сам пользователь, не имеющий доступа к определенному Internet-ресурсу из-за настроек межсетевого экрана, может использовать данный метод для обхода правил межсетевого экрана. Более простой случай, наглядно иллюстрирующий данную уязвимость, — это использование пользователями личных флеш-накопителей, которые могут передать на рабочую станцию или сервер вредоносную программу или вирус.

Пользователь может быть уязвимым для определенных атак, если он не обновляет свои клиентские приложения. Ни для кого не секрет, что все современные программы постоянно обновляются. И одной из целей этих обновлений является закрытие брешей в безопасности, исправление уязвимых мест в алгоритме работы программы. Если своевременно не обновлять приложение, высока вероятность, что злоумышленник воспользуется открытой ранее уязвимостью.

Для повышения безопасности информации, для обеспечения защиты рабочих станций и серверов необходимо выполнять следующие рекомендации:

- Использование сильных паролей. Сильный пароль — комбинация символов, состоящая не менее чем из восьми символов. Обязательно должны использоваться одновременно буквы верхнего и нижнего регистра, цифры и специальные символы, такие как “@”, “#”, “!” и так далее.
- Разграничение доступа в системе рабочей станции и сервера, хотя бы на уровне «пользователь — администратор».
- Своевременное обновление приложений и операционной системы для исправления уязвимостей.
- Использовать программный или аппаратный межсетевой экран с конфигурацией, отвечающей требованиям безопасности.

– Ограничить или запретить вовсе использование посторонних устройств, а использовать только те, что разрешены для применения исключительно на территории организации/предприятия.

В ходе этой статьи были рассмотрены некоторые уязвимости рабочих станций и серверов, также были описаны рекомендации для предупреждения атак с использованием данных уязвимостей.